REMARKS

The Examiner is thanked for the performance of a thorough search. By this response, Claims 1, 3–6, 9, 10, 12, 14, 16–20, 24–26, and 28–31 have been amended. Claims 32–42 have been added. Claims 15, 21, 22, and 27 have been canceled. Hence, Claims 1–14, 16–20, and 24–42 are pending in this application.

All issues raised in the Office Action are addressed hereinafter.

I. CLAIM REJECTIONS BASED ON 35 U.S.C. § 112

Claims 22 and 25 stand rejected under 35 U.S.C. § 112, first paragraph, as allegedly failing to comply with the enablement requirement. Specifically, the Office Action alleged that Claims 22 and 25 contained improper "single means plus function claims."

Claim 22 is presently canceled, thereby obviating the rejection as to Claim 22. Claim 25 presently recites seven specific "means for" clauses. Applicants therefore submit that Claim 25 complies with the enablement requirement under 35 U.S.C. § 112. Removal of the rejection as to both claims is requested.

II. CLAIM REJECTIONS BASED ON 35 U.S.C. § 102

Claims 1–32 are rejected under 35 U.S.C. § 102(2) as allegedly anticipated by U.S. Patent No. 7,127,524 B1 to Renda et al. (hereinafter *Renda*). Applicants traverse the rejection. Reconsideration is respectfully requested.

To anticipate under 35 U.S.C. § 102, a reference must show all elements, steps or limitations of a claim, arranged as in the claim. An anticipation rejection is unsupported or overcome if a reference is missing even one element, step, or limitation. *See Connell v. Sears, Roebuck & Co.*, 722 F.2d 1542, 1548, 220 USPQ 193, 198 (Fed. Cir. 1983).

INDEPENDENT CLAIM 1

Claim 1, as set forth in the listing of claims, clarifies that the method features:

> in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
> determining a user identifier associated with the network device that has caused a security event in the network;
> **in response** to the security event, **causing the network device to acquire** a new network address that is selected from a **second subset of addresses within a second specified pool associated with suspected malicious network users**;
> wherein the second subset of addresses is different from the first subset of addresses; and
> configuring one or more security restrictions with respect to the new network address.

For example, a security controller implementing the steps of Claim 1 may receive information identifying a "security event," such as high network usage or an illegal user action. *See, e.g., Rayes et al.* U.S. Serial No. 10/688,051, at ¶ [0016] (incorporated into Applicants' Specification by reference) ("Security event is any network event that has security implication. . . . For example, an illegal user action will constitute a security event and will cause an alarm. A high utilization of some network resource will also constitute a security event because it may be caused by some malicious activities."). The security controller may determine that a certain network device caused the security event, and that a certain user is associated with the network device. The certain network device already has a DHCP-assigned network address selected from a normal pool of addresses (an example of "a first network address assigned from a first subset of addresses" in the claim). *See, e.g.*, Specification at ¶ [0029]. Any user of a network device with an address in this normal pool of addresses may use the network in a normal manner.

In response to the security event, however, the security controller may effectively quarantine the certain user. *See, e.g.*, Specification at ¶ [0033]. The security controller accomplishes this by forcing the certain network device to acquire a new network address from the DHCP server (an example of "causing the network device to acquire a new network address"

in the claim). This new network device is selected from a different pool of addresses than the normal pool of address (an example of "a second set of addresses" in the claim). *See*, *e.g.*, Specification at ¶ [0029]. Any user of a network device with an address in this normal pool of addresses may use the network in a more restricted manner because the security controller "configures one or more security restrictions with respect to the new network address."

By contrast, *Renda* discloses a system and method of controlling access to various resources on a network by "determining whether a user of [a] device with [a certain] MAC address has permission to access a destination." *Renda* at col. 3, lines 60–67. The system relies on an authentication server that intercepts and redirects communications to various resources. *Renda* at col. 4. Renda contemplates that "to prevent conflicts" that may arise when a user moves to a different access point, the user may be identified by an IP address "instead of a translated address." *Renda* at col. 4, lines 24–32. As is known in the art, a network device may obtain an IP address via DHCP. Thus, *Renda* discusses how an authentication server may authenticate and respond to a network device that requests an IP address via DHCP. *Renda* at col. 4, lines 24–32, and col. 14 line 55–col. 16, line 56.

A. **Renda** *fails to disclose "in response to the security event, causing the network device to acquire a new network address"*

Renda does not teach or suggest "in response to the security event, causing the network device to acquire a new network address," as recited in Claim 1. The Office Action only vaguely alleges that *Renda* discusses a "security event" in col. 9, lines 45–55, col. 10, lines 4–26, col. 23, lines 31–33, and col. 24, lines 3–9. However, the Office Action fails to allege what feature of *Renda* discussed in these passages is a "security event." Applicants have thus been required to engage in guesswork to determine the meaning of the Office Action and believe that *Renda* fails to disclose a security event at all.

However, regardless of whether or not *Renda* discloses a "security event," the acquisition of a new network address in *Renda* does not occur "in response to [a] security event" as claimed. Rather, the only acquisition of a new network address discussed in *Renda* occurs in response to a network device that, **on its own initiative**, requests a new IP address via a DHCP request. *See*, *e.g.*, *Renda* at col. 15 lines, 11–14 and col. 25, lines 29–34. Thus, while *Renda* teaches that the

authentication server may receive a DHCP request or a request to renew a lease, *Renda* says nothing about this request being "caused" by or "in response" to anything, and certainly not "in response to [a] security event."

Furthermore, *Renda* does not disclose "causing the network device to acquire a new network address." One skilled in the art would understand that a network device "acquir[ing] a new network device," as opposed to "receiving a new network address" entails the network device actively requesting a new network address. However, *Renda*'s authentication server does not force a network device "to acquire" a new network address by, for example, forcing the network device to send out a new DHCP request. Rather, *Renda* teaches that when a network device moves to a new access point, the network device, on its own initiative, sends a DHCP request so as to acquire a new network address.

B. Renda *fails to disclose "a second subset of addresses within a second specified pool associated with suspected malicious network users"*

Also, *Renda* does not disclose "a second subset of addresses within a second specified pool associated with suspected malicious network users." As is well-known with DHCP, *Renda* discusses that a DHCP manager may assign a DHCP client an address "from a pool of IP addresses DHCP manager 284 maintains as provided by a system manager" or "in another embodiment, . . . an IP address selected randomly from a large address space." *Renda* at col. 16, lines 15–22. However, at no point does *Renda* disclose assigning "a new network address that is selected from a **second subset of addresses** within a **second specified pool**." In *Renda*, rather, a system manager specifies **only one** pool of IP addresses and a DHCP manager assigns addresses from **only one** DHCP address pool.

Nor does *Renda* teach a "second specified pool" that is "**associated with suspected malicious network users**." The only pool of addresses from which *Renda* contemplates assigning addresses is a subset of addresses for normal network operations, not suspected malicious network users.

For at least the foregoing reasons, *Renda* fails to teach or suggest at least one feature of independent Claim 1. Therefore, *Renda* does not anticipate Claim 1 under 35 U.S.C. § 102. Reconsideration is respectfully requested.

INDEPENDENT CLAIM 14

Claim 14, as set forth in the listing of claims, clarifies that the method features:

> in a security controller that is coupled, through a network, to a network device having a first network address assigned from a first subset of addresses within a first specified pool associated with normal network users:
> receiving information identifying a security event in the network;
> correlating the security event information with network user information to result in determining a network user associated with the network device that caused the security event;
> in response to receiving the information identifying the security event, placing the user in an elevated risk security group by causing the network device to acquire a new network address that is selected from a second subset of addresses within a second specified pool associated with suspected malicious network users;
> wherein the second subset of addresses is different from the first subset of addresses;
> configuring one or more security restrictions with respect to the new network address;
> **determining whether a malicious act caused the security event**;
> if a malicious act caused the security event, then providing information about the security event or malicious act to a security decision controller;
> if a malicious act did not cause the security event, then **removing the user from the elevated risk group**.

Thus, a security controller may begin implementing the steps of Claim 14 in much the same manner as it implements Claim 1. After assigning a network device to a new network address, however, the security controller may then determine whether or not the security event was caused by a malicious act. If the event was caused by a malicious act, a security decision controller may take further actions. If not, the network device may be removed from the elevated risk group.

C. Renda *does not teach "determining whether a malicious act caused [a] security event."*

By contrast, *Renda* says nothing about "determining whether a malicious act caused [a] security event." *Renda*, in fact, says nothing about a "malicious act." The Office Action alleges that *Renda* discloses such a step because *Renda* discloses identifiers and privilege records that may be "necessary for the determination on whether or not to allow a user requesting access to the network resources." However, a "determination on whether or not to allow a user requesting access to the network resources" is not the same as "determining whether a malicious act caused [a] security event."

Aside from the fact that Office Action fails to specifically identify what aspect of *Renda* is the "security event" and what aspect is the "malicious act," the Office Action appears to improperly assume that a security event is necessarily caused by a malicious act. In fact, there may be many reasons why a security event occurs, not all of which are "malicious." For example, a security event may have been triggered through user error. Thus, Claim 14 features a step of determining whether a malicious act caused a security event.

Furthermore, the Office Action improperly assumes that just because *Renda* may disclose resources that may be used for a certain step, that *Renda* actually teaches one to perform the step. Just because *Renda* discloses identifiers and privileges, does not mean that *Renda* teaches one skilled in the art an actual step of determining whether a malicious act caused a security event, even if the disclosed resources could be used to make such a determination.

D. Renda *does not teach "removing the user from the elevated risk group."*

Also, *Renda* fails to teach or suggest "if a malicious act did not cause the security event, then **removing the user from the elevated risk group**." *Renda* does not, for example, discuss assigning a user to second pool of IP addresses after the security event, and then removing the user from that second pool of IP addresses once it is determined that the security event was caused by a non-malicious act.

The Office Action again alleges that *Renda* teaches this step because *Renda* discloses identifiers and privilege records that may be "necessary for the determination on whether or not to allow a user requesting access to the network resources." However, neither the cited passages

nor the logic relied upon in the Office Action for rejecting this step teaches to remove a user from an elevated risk group. In fact, the Office Action fails to even identify in *Renda* an elevated risk group from which a user may be removed.

For at least the reasons discussed for Claim 1, as well as reasons discussed above, *Renda* fails to teach or suggest at least one limitation of independent Claim 14. Therefore, *Renda* does not anticipate Claim 14 under 35 U.S.C. § 102. Reconsideration is respectfully requested.

DEPENDENT CLAIMS 2–13, 15–17

Claims 2–13 and 16–17 depend from Claims 1 and 14, respectively, and include each of the above-quoted features by dependency. Thus, *Renda* also lacks at least one feature found in Claims 2–13 and 16–17. Therefore, *Renda* does not anticipate Claims 2–13 and 16–17. Also, Claim 15 is presently canceled, thereby obviating the rejection as to Claim 15. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 2–13 and 16–17 recites at least one feature that independently renders it patentable. For example Claim 3 recites a step of "**resetting a port** that is coupled to the network device to prompt a user to command the network device to request a new network address using DHCP." The passages of *Renda* cited in the Office Action neither teach nor suggest "resetting a port."

As another example, Claim 4 recites "issuing a **DHCP FORCE_RENEW** message to the network device." Again, the passages of *Renda* cited in the Office Action as teaching this step neither teach nor suggest using a **DHCP FORCE_RENEW** message to cause a network device to acquire a new network address.

To expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 2–13 and 16–17 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

INDEPENDENT CLAIMS 18–20 AND 24–26

Independent Claims 18–20 and 24–26 also recites the features quoted for Claim s1 and 14, respectively, although Claims 18–20 and 24–26 are expressed in another format. Claims 18–

20 and 24–26 have all the features described above for Claims 1 and 14, respectively, and therefore Claims 18–20 and 24–26 are allowable over *Renda* for the same reasons given above for Claims 1 and 14, respectively. Reconsideration is respectfully requested.

DEPENDENT CLAIMS 21–23 AND 27–32

Claims 27–29 and 30–32 depend from Claims 26 and 20, respectively, and include each of the above-quoted features by dependency. Thus, *Renda* also lacks at least one feature found in Claims 27–29 and 30–32. Therefore, *Renda* does not anticipate Claims 27–29 and 30–32. Also, Claims 21–23 are presently canceled, thereby obviating the rejection as to Claims 21–23. Reconsideration of the rejection is respectfully requested.

In addition, each of Claims 27–29 and 30–32 recites at least one feature that independently renders it patentable. To expedite prosecution in light of the fundamental differences already identified, further arguments for each independently patentable feature of Claims 27–29 and 30–32 are not provided at this time. Applicants reserve the right to further point out the differences between the cited art and the novel features recited in the dependent claims.

III. ADDED CLAIMS / AMENDMENTS

The added claims and amendments to the claims do not add any new matter to this application. The amendments to Claims 1, 14, 18–20, and 24–26 are supported by at least ¶ [0029] of the Specification. The amendments to Claim 18 and 24 are further supported by ¶ [0058] of the Specification. All other amendments to the claims address informalities. The amendments to the claims were made to improve the readability and clarity of the claims and not necessarily for any reason related to patentability.

Added Claims 32–42 recite computer-readable storage media carrying instructions for or apparatuses comprising means for performing the methods recited in Claims 3, 4, 7, 15, or 17. Thus, Claims 32–42 do not introduce any new subject matter. Furthermore, Claims 32–42 are patentable over the cited references for the same reasons as Claims 3, 4, 7, 15, or 17.

IV. CONCLUSION

For the reasons set forth above, all of the pending claims are now in condition for allowance. The Examiner is respectfully requested to contact the undersigned by telephone relating to any issue that would advance examination of the present application.

A petition for extension of time, to the extent necessary to make this reply timely filed, is hereby made. If applicable, a check for the petition for extension of time fee and other applicable fees is enclosed herewith. If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: January 31, 2008

/KarlTRees#58983/
Karl T. Rees, Reg. No. 58,983

2055 Gateway Place, Suite 550
San Jose, CA 95110

(408) 414-1233

Facsimile: (408) 414-1076